## IC ON THE RECORD



Go to LinkPop-upView Separately

**DNI Statement:**

**Why the Intelligence Community Seeks to Understand Online Communication Tools & Technologies**

**October 4, 2013**

Recently published news articles discuss the Intelligence Community's interest in tools used to facilitate anonymous online communication. The articles accurately point out that the Intelligence Community seeks to understand how these tools work and the kind of information being concealed.

However, the articles fail to make clear that the Intelligence Community's interest in online anonymity services and other online communication and networking tools is based on the undeniable fact that these are the tools our adversaries use to communicate and coordinate attacks against the United States and our allies.

The articles fail to mention that the Intelligence Community is only interested in communication related to valid foreign intelligence and counterintelligence purposes and that we operate within a strict legal framework that prohibits accessing information related to the innocent online activities of US citizens.

Within our lawful mission to collect foreign intelligence to protect the United States, we use every intelligence tool available to understand the intent of our foreign adversaries so that we can disrupt their plans and prevent them from bringing harm to innocent Americans.

In the modern telecommunications era, our adversaries have the ability to hide their messages and discussions among those of innocent people around the world. They use the very same social networking sites, encryption tools and other security features that protect our daily online activities.

Americans depend on the Intelligence Community to know who and what the threats are, and where they come from. They want us to provide policy makers with the information necessary to keep our nation safe, and they rightfully want us to do this without compromising respect for the civil liberties and privacy of our citizens.

Many of the recent articles based on leaked classified documents have painted an inaccurate and misleading picture of the Intelligence Community. The reality is that the men and women at the National Security Agency and across the Intelligence Community are abiding by the law, respecting the rights of citizens and doing everything they can to help keep our nation safe.

James R. Clapper
Director of National Intelligence

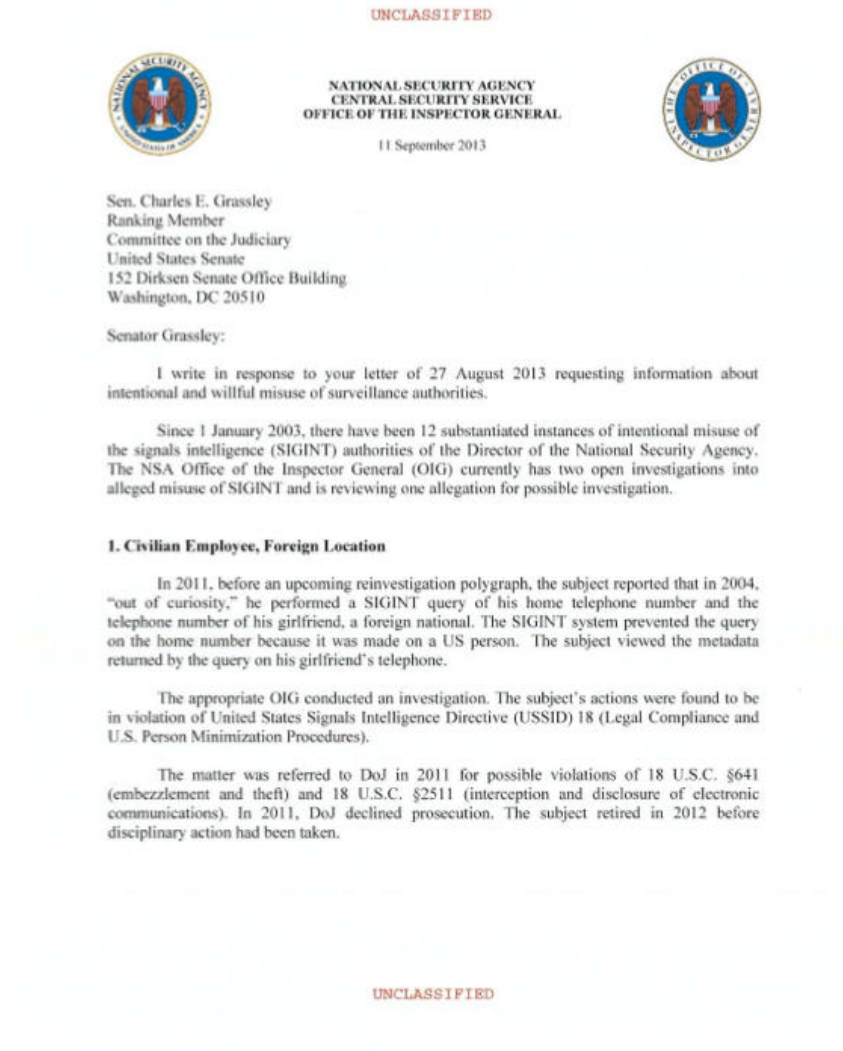
- #statement
- #online communications
- #NSA
- 4 months ago
- 16
- Permalink

Share

Short URL
http://tmblr.co/ZZQjsqw

TwitterFacebookPinterestGoogle+


Zoom Info



UNCLASSIFIED

NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE
OFFICE OF THE INSPECTOR GENERAL

11 September 2013

Sen. Charles E. Grassley
Ranking Member
Committee on the Judiciary
United States Senate
152 Dirksen Senate Office Building
Washington, DC 20510

Senator Grassley:

I write in response to your letter of 27 August 2013 requesting information about intentional and willful misuse of surveillance authorities.

Since 1 January 2003, there have been 12 substantiated instances of intentional misuse of the signals intelligence (SIGINT) authorities of the Director of the National Security Agency. The NSA Office of the Inspector General (OIG) currently has two open investigations into alleged misuse of SIGINT and is reviewing one allegation for possible investigation.

**1. Civilian Employee, Foreign Location**

In 2011, before an upcoming reinvestigation polygraph, the subject reported that in 2004, "out of curiosity," he performed a SIGINT query of his home telephone number and the telephone number of his girlfriend, a foreign national. The SIGINT system prevented the query on the home number because it was made on a US person. The subject viewed the metadata returned by the query on his girlfriend's telephone.

The appropriate OIG conducted an investigation. The subject's actions were found to be in violation of United States Signals Intelligence Directive (USSID) 18 (Legal Compliance and U.S. Person Minimization Procedures).

The matter was referred to DoJ in 2011 for possible violations of 18 U.S.C. §641 (embezzlement and theft) and 18 U.S.C. §2511 (interception and disclosure of electronic communications). In 2011, DoJ declined prosecution. The subject retired in 2012 before disciplinary action had been taken.

UNCLASSIFIED

Zoom Info

**NSA Inspector General's Letter to Senator Charles Grassley**

*Letter to Senator Grassley from the National Security Agency Inspector General dated September 11, 2013.*

Download the full letter from NSA.gov

- #NSA
- #Congressional Oversight
- #Inspector General
- #Senator Grassley
- #oversight

- 4 months ago
- 4
- Permalink

Share

Short URL
http://tmblr.co/ZZQjsqw

TwitterFacebookPinterestGoogle+

Go to LinkPop-upView Separately

**Remarks as delivered by Deputy Attorney General, James Cole**

*Open Hearing on Foreign Intelligence Surveillance Authorities, U. S. Senate Select Committee on Intelligence*

*Thursday, September 26, 2013*

*216 Hart Senate Office Building, Capitol, Washington DC*

---

Thank you, Chairman Feinstein, Vice Chairman Chambliss, distinguished members of the committee, for inviting us here today to talk about NSA's 215 business records program and Section 702 of FISA. I'm going to try and be brief and just focus my opening remarks on the 215 program.

NSA's 215 program involves the collection of metadata from telephone calls, including the number that was dialed, the date and time of the call and the length of the call.

The metadata collection does not include the content of any phone calls, any names, addresses or financial information of any party to a call or cell site location information. Moreover, the vast majority of the data obtained by NSA under this program is never reviewed.

The government can only search the data if it has a reasonable, articulable suspicion that the phone number being searched is associated with certain terrorist organizations.

Read More

- #Testimony
- #James Cole
- #Section 702
- #Section 215
- #FISA
- #FISC
- #Congressional Oversight
- #Department of Justice

- 4 months ago
- 7
- Permalink

Share

Short URL
http://tmblr.co/ZZQjsqw-

TwitterFacebookPinterestGoogle+


Go to LinkPop-upView Separately

**Remarks as delivered by General Keith Alexander, Director of the National Security Agency**

*Open Hearing on Foreign Intelligence Surveillance Authorities, U. S. Senate Select Committee on Intelligence*

*Thursday, September 26, 2013*

*216 Hart Senate Office Building, Capitol, Washington DC*

---

Chairman Feinstein, Vice Chairman Chambliss, distinguished members of the committee, I am privileged today to represent the work of the dedicated professionals at the National Security Agency, who employ the authorities provided by Congress, the courts and the executive branch to help defend this nation. If we are to have a serious debate about how NSA conducts its business, we need to step away from sensational headlines and focus on the facts.

Today, I'd like to present facts about four key areas: who we are in terms of both our mission and our people; what we do — adapt to technology and the threat, take direction from political leadership, use lawful programs, tools, and ensure compliance; I'd like to cover what we have accomplished for our country with the tools we have been authorized; and where do we go from here.

Read More

- #Testimony
- #Keith Alexander
- #NSA
- #Section 702
- #Section 215
- #FISA
- #FISC

- 4 months ago
- 7
- Permalink

Share

Short URL
http://tmblr.co/ZZQjsqw-

TwitterFacebookPinterestGoogle+

# TESTIMONY

Go to LinkPop-upView Separately

**Remarks as prepared for delivery by Director of National Intelligence James R. Clapper**

*Open Hearing on Foreign Intelligence Surveillance Authorities, U. S. Senate Select Committee on Intelligence*

*Thursday, September 26, 2013*

*216 Hart Senate Office Building, Capitol, Washington DC*

---

Chairman Feinstein, Vice Chairman Chambliss, and distinguished members of the Committee.

Thank you for having us here today, to talk about the way ahead, occasioned by the dramatic revelations about intelligence collection programs since their unauthorized disclosure, and about the steps we're taking to make these programs more transparent, while still protecting our national security interests.

I'm joined today by the Deputy Attorney General, Jim Cole, and the Director of the National Security Agency, General Keith Alexander.

This hearing is a key part of the discussion our nation needs, about legislation that provides the Intelligence Community with authorities, both to collect critical foreign intelligence, and to protect privacy and civil liberties.

We, all of us, in the IC, are very much aware that the recent unauthorized disclosures have raised serious concerns, both here in Congress, and across the nation, about our intelligence activities.

We know that the public wants both to understand how its Intelligence Community uses its special tools and authorities, and to judge whether we can be trusted to use them appropriately. We believe we have been lawful, and that the rigorous oversight we've operated under has been effective. So we welcome this opportunity to make our case to the public.

As we engage in this discussion, I think it's also important that our citizens know that the unauthorized disclosure of the details of these programs has been extremely damaging.

From my vantage, these disclosures are threatening our ability to conduct intelligence, to keep our country safe. There is no way to erase or make up for the damage that we know has already been done, and we anticipate even more, as we continue our assessment.

Before the unauthorized disclosures, we were always conservative about discussing specifics of our collection programs, based on the truism that the more adversaries know about what we're doing, the more they can avoid our surveillance. But the disclosures, for better or worse, have lowered the threshold for discussing these matters in public. So, to the degree that we can discuss them, we will.

However, this public discussion should be based on an accurate understanding of the Intelligence Community: Who we are, what we do, and how we're overseen.

In the last few months, the manner in which our activities have been characterized has often been incomplete, inaccurate, or misleading.

I believe that most Americans realize the Intelligence Community exists to collect the vital intelligence that helps protect our nation from foreign threats. We focus on uncovering the secret plans and intentions of our foreign adversaries.

But what we do not do is spy unlawfully on Americans; or for that matter, spy indiscriminately on the citizens of any country.

We only "spy" for valid foreign intelligence purposes, as authorized by law, and with multiple layers of oversight, to ensure that we do not abuse our authorities. Unfortunately, this reality has been obscured in the current debate. And for some, this has led to a lowering of trust in the Intelligence Community.

I do understand the concerns on the part of the public. I'm a Vietnam veteran, and I remember – as Congressional investigations of the 1970s later disclosed – that some intelligence programs back then were carried out for domestic political purposes, without proper legal authorization or oversight.

But I can assure the American people that the Intelligence Community of today is not like that at all. We operate within a robust framework of strict rules and rigorous oversight, involving all three branches of government.

Another useful historical perspective: During the Cold War, the Free World and the Soviet bloc had mutually exclusive telecommunications systems, which made foreign collection easier to distinguish. Now, world telecommunications are unified, intertwined with hundreds of millions of innocent people conducting billions of innocent transactions, while a much lesser number of nefarious adversaries are trying to do harm on the same network. Our challenge is to distinguish very precisely, between those two groups of communicants.

If we had an alarm bell that went off whenever one terrorist communicated with another terrorist, our jobs would be much easier. But that capability doesn't exist in the real world.

Over the past three months, I've declassified and publicly released a series of documents related to both Section 215 of the PATRIOT Act and Section 702 of the Foreign Intelligence Surveillance Act. I did that to facilitate informed public debate about the important intelligence collection programs that operate under these authorities.

I felt that in light of the unauthorized disclosures, the public interest in these documents far outweighed the potential additional damage to national security.

These documents let our citizens see the seriousness, thoroughness, and rigor with which the FISA Court exercises its responsibilities. They also reflect the Intelligence Community's commitment to uncovering, reporting, and correcting any compliance matters that occur.

However, even in these documents, we've had to redact certain information to protect sensitive sources and methods, such as particular targets of surveillance.

We'll continue to declassify more documents. That's what the American people want, it's what the President has asked us to do, and I personally believe it's the only way we can reassure our citizens that their Intelligence Community is using its tools and authorities appropriately.

The rules and oversight that govern us ensure we do what the American people want us to do: Protect our nation's security and our people's liberties. I will repeat: We do not spy on anyone except for valid foreign intelligence purposes, and we only work within the law.

On occasion, we've made mistakes – some quite significant. But these are usually caused by human error or technical problems. And whenever we've found mistakes, we've reported, addressed, and corrected them.

The National Security Agency specifically, as part of the U.S. Intelligence Community broadly, is an honorable institution. The men and women who do this sensitive work are honorable people, dedicated to conducting their mission lawfully, and are appalled by any wrongdoing.

They, too, are citizens of this Nation who care just as much about privacy and constitutional rights as the rest of the public. They should be commended for their crucial and important work in protecting the people of this country, which has been made all the more difficult by the torrent of unauthorized, damaging disclosures.

That all said, we in the IC stand ready to work in partnership with you, to adjust foreign surveillance authorities, to further protect our privacy and civil liberties.

I think there are some principles we already agree on:

1. We must always protect our sources, methods, targets, partners, and liaison relationships.
2. We must do a better job in helping the American people understand what we do, why we do it, and, most importantly, the oversight of our activities.
3. We must take every opportunity to demonstrate our commitment to respecting the civil liberties and privacy of every American.

But, we also have to remain mindful of the potentially negative long-term impact of over-correcting the authorizations granted to the Intelligence Community.

As Americans, we face an unending array of threats to our way of life. We need to sustain our ability to detect those threats.

We welcome a balanced discussion about national security and civil liberties. But it's not an either/or situation; we need to continue to protect both.

Thank you. We look forward to answering your questions.

___

DNI Clapper's as delivered remarks are available via DNI.gov.

- #DNI Clapper
- #testimony
- #FISA
- #Section 702
- #Section 215
- #FISC
- #Congressional Oversight

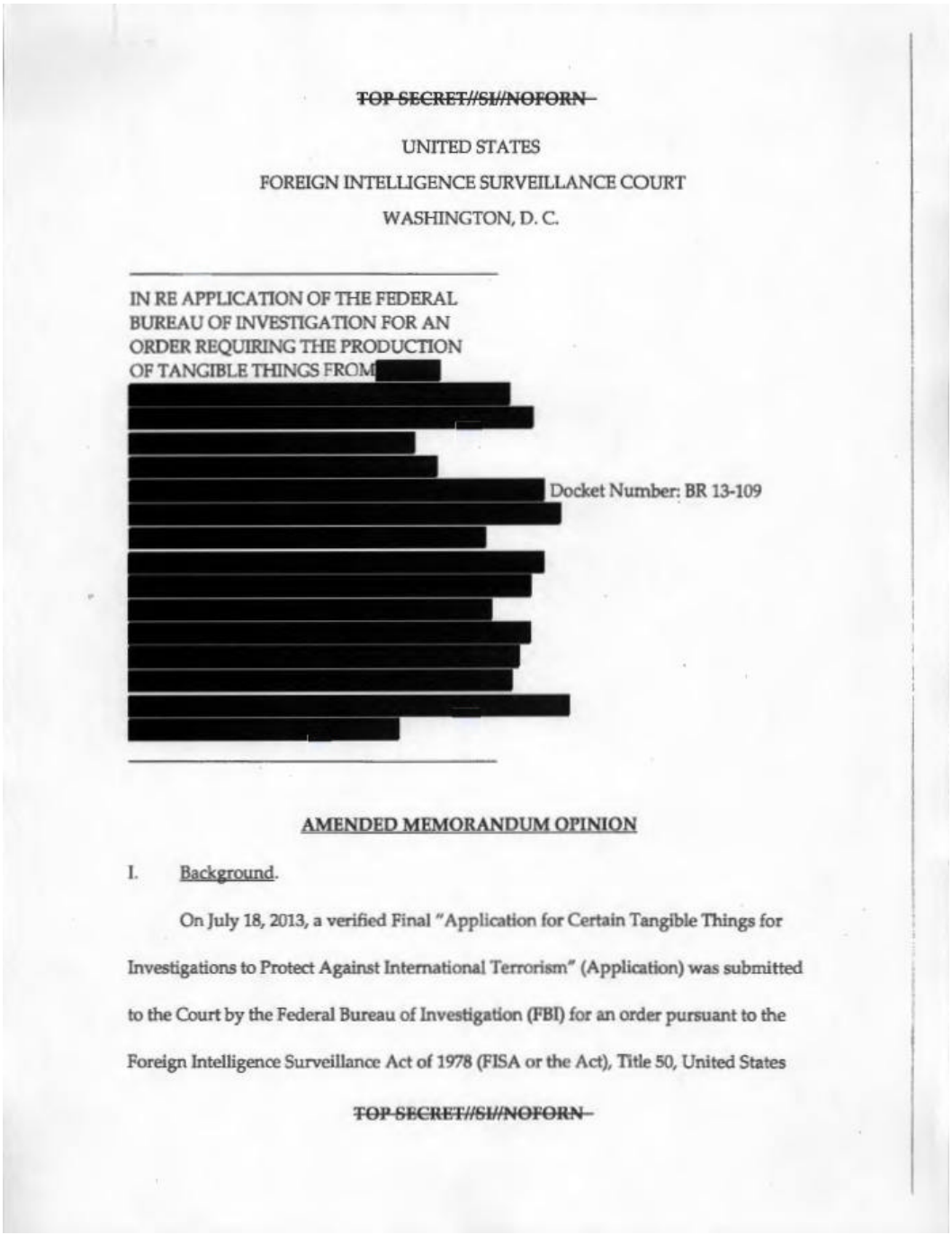
- 4 months ago
- 6
- Permalink

Share

Short URL
http://tmblr.co/ZZQjsqw-

TwitterFacebookPinterestGoogle+


Zoom Info



~~TOP SECRET//SI//NOFORN~~

UNITED STATES

FOREIGN INTELLIGENCE SURVEILLANCE COURT

WASHINGTON, D. C.

IN RE APPLICATION OF THE FEDERAL BUREAU OF INVESTIGATION FOR AN ORDER REQUIRING THE PRODUCTION OF TANGIBLE THINGS FROM [redacted]

Docket Number: BR 13-109

AMENDED MEMORANDUM OPINION

I. Background.

On July 18, 2013, a verified Final "Application for Certain Tangible Things for Investigations to Protect Against International Terrorism" (Application) was submitted to the Court by the Federal Bureau of Investigation (FBI) for an order pursuant to the Foreign Intelligence Surveillance Act of 1978 (FISA or the Act), Title 50, United States

~~TOP SECRET//SI//NOFORN~~

Zoom Info

**Release of Previously Classified August 29, 2013 Foreign Intelligence Surveillance Court Opinion**

Today the Foreign Intelligence Surveillance Court released a previously classified opinion reauthorizing the collection of bulk telephony metadata under Section 215 of the USA Patriot Act. The opinion affirms that the bulk telephony metadata collection is both lawful and constitutional. The release of this opinion is consistent with the President's call for more transparency on these valuable intelligence programs.

**Download:** Eagan Order, Foreign Intelligence Surveillance Court

- #declassified
- #judicial oversight
- #fisa
- #fisc
- #patriot act

- 5 months ago
- 10
- Permalink

Share

Short URL
http://tmblr.co/ZZQjsqvJ

TwitterFacebookPinterestGoogle+


Go to LinkPop-upView Separately

**DNI Clapper Declassifies Intelligence Community Documents Regarding Collection Under Section 501 of the Foreign Intelligence Surveillance Act (FISA)**

**September 10, 2013**

In June of this year, President Obama directed me to declassify and make public as much information as possible about certain sensitive intelligence collection programs undertaken under the authority of the Foreign Intelligence Surveillance Act (FISA) while being mindful of the need to protect national security. Consistent with this directive, today I authorized the declassification and public release of a number of documents pertaining to the Government's collection of bulk telephony metadata under Section 501 of the FISA, as amended by Section 215 of the USA PATRIOT Act. These documents were properly classified, and their declassification is not done lightly. I have determined, however, that the harm to national security in these circumstances is outweighed by the public interest.

Release of these documents reflects the Executive Branch's continued commitment to making information about this intelligence collection program publicly available when appropriate and consistent with the national security of the United States. Some information has been redacted because these documents include discussion of matters that continue to be properly classified for national security reasons and the harm to national security would be great if disclosed. These documents will be made available at the website of the Office of the Director of National Intelligence (www.dni.gov), and on the recently established public website dedicated to fostering greater public visibility into the intelligence activities of the Government (IContheRecord.tumblr.com).

The documents released today were provided to Congress at the time of the events in question and include orders and opinions from the Foreign Intelligence Surveillance Court (FISC), filings with that court, an Inspector General Report, and internal NSA documents. They describe certain compliance incidents that were discovered by NSA, reported to the FISC and the Congress, and resolved four years ago. They demonstrate that the Government has undertaken extraordinary measures to identify and correct mistakes that have occurred in implementing the bulk telephony metadata collection program – and to put systems and processes in place that seek to prevent such mistakes from occurring in the first place.

More specifically, in response to the compliance incident identified in 2009, the Director of NSA instituted a number of remedial and corrective steps, including conducting a comprehensive "end-to-end" review of NSA's handling of telephony metadata obtained under Section 501. This comprehensive review identified additional incidents where NSA was not complying with aspects of the FISC's orders.

The compliance incidents discussed in these documents stemmed in large part from the complexity of the technology employed in connection with the bulk telephony metadata collection program, interaction of that technology with other NSA systems, and a lack of a shared understanding among various NSA components about how certain aspects of the complex architecture supporting the program functioned. These gaps in understanding led, in turn, to unintentional misrepresentations in the way the collection was described to the FISC. As discussed in the documents, there was no single cause of the incidents and, in fact, a number of successful oversight, management, and technology processes in place operated as designed and uncovered these matters.

Upon discovery of these incidents, which were promptly reported to the FISC, the Court, in 2009, issued an order requiring NSA to seek Court approval to query the telephony metadata on a case-by-case basis, except when necessary to protect against an imminent threat to human life. Thereafter, NSA completed its end-to-end review and took several steps to remedy these issues, including making technological fixes, improving training, and implementing new oversight procedures. These remedial steps were then reported to the Court, and in September 2009, the Court lifted the requirement for NSA to seek approval to query the telephony metadata on a case-by-case basis and has since continuously reauthorized this program. The Intelligence and Judiciary Committees were informed of the compliance incidents beginning in February 2009 and kept apprised of the Government's corrective measures throughout the process, including being provided copies of the Court's opinions, the Government's report to the Court, and NSA's end-to-end review.

Upon discovery of these issues in 2009, NSA also recognized that its compliance and oversight infrastructure had not kept pace with its operational momentum and the evolving and challenging technological environment in which it functioned. Therefore NSA, in close coordination with the Office of the Director of National Intelligence and the Department of Justice, also undertook significant steps to address these issues from a structural and managerial perspective, including thorough enhancements to its compliance structure that went beyond this specific program. For example, in 2009, NSA created the position of the Director of Compliance, whose sole function is to keep all of NSA's mission activities consistent with the law and applicable policies and procedures designed to protect U.S. person privacy by strengthening NSA's compliance program across NSA's operational and technical personnel. NSA also added additional technology-based safeguards, implemented procedures to ensure accuracy and precision in FISC filings, and initiated regular detailed senior leadership reviews of the compliance program. NSA has also enhanced its oversight coordination with the Office of the Director of National Intelligence and the Department of Justice.

Since 2009, the Government has continued to increase its focus on compliance and oversight. Today, NSA's compliance program is directly supported by over three hundred personnel, which is a fourfold increase in just four years. This increase was designed to address changes in technology and authorities and reflects a commitment on the part of the Intelligence Community and the rest of the Government to ensuring that intelligence activities are conducted responsibly and subject to the rule of law. NSA's efforts have proven successful in its implementation of the telephony metadata collection program since the changes made in 2009. Although there have been a handful of compliance incidents each year, these were the result of human error or provider error in individual instances and were not the result of systemic misunderstandings or problems of the type discovered in 2009. Each of these individual incidents upon identification were immediately reported to the FISC and remedied.

Moreover, the FISC in September of 2009 relieved the Government of its requirement to seek Court approval to query the metadata on a case-by-case basis and has continued to reauthorize this program. Indeed, in July of this year the FISC once again approved the Government's request for reauthorization.

The documents released today are a testament to the Government's strong commitment to detecting, correcting, and reporting mistakes that occur in implementing technologically complex intelligence collection activities, and to continually improving its oversight and compliance processes. As demonstrated in these documents, once compliance incidents were discovered in the telephony metadata collection program, additional checks, balances, and safeguards were developed to help prevent future instances of non-compliance.

James R. Clapper, Director of National Intelligence

---

**Cover Letters for Congressional Submissions**

March 5, 2009 — Cover Letter to Chairman of the Intelligence and Judiciary Committees

*Cover letter submitting several Foreign Intelligence Surveillance Court (FISC) opinions and Government filings relating to the Government's discovery and remediation of compliance incidents in its handling of bulk telephony metadata under docket number BR 08-13, described below.*

September 3, 2009 — Cover Letter to Chairman of the Intelligence and Judiciary Committees

*Cover letter submitting the Government's report to the Court and NSA's end-to-end review describing its investigation and remediation of compliance incidents in its handling*

*of bulk telephony metadata under docket number BR-09-09, described below.*

**Docket Number BR 06-05**

May 24, 2006 — Order from the Foreign Intelligence Surveillance Court

*Order of the FISC approving the Government's request for authorization to collect bulk telephony metadata under Section 501 of FISA.*

**Docket Number BR 08-13**

December 12, 2008 — Supplemental Opinion from the Foreign Intelligence Surveillance Court

*Opinion of the FISC concluding that the production of bulk telephony metadata records pursuant to Section 501 of FISA is not inconsistent with Sections 2702 and 2703 of Title 18 of the United States Code.*

January 28, 2009 — Order Regarding Preliminary Notice of Compliance Incident Dated January 15, 2009 from the Foreign Intelligence Surveillance Court

*Order of the FISC directing the Government to provide additional information regarding its identification and notification that NSA had improperly queried the bulk telephony metadata by using an automated "alert list" process that resulted in the use of selectors that had not been individually reviewed and determined to meet he required reasonable articulable suspicion standard.*

February 12, 2009 — Memorandum of the United States in response to the Court's Order Dated January 28, 2009, with attachments:

*Memorandum of the Government providing additional information relating to the compliance incident described directly above and describing additional oversight mechanisms deployed by the Government following identification of this compliance incident.*

- (Tab 1) Declaration of Lieutenant General Keith B. Alexander signed February 13, 2009
  - Attachment A: Internal NSA Email
  - Attachment B: NSA Interim Procedures
  - Attachment C: Former Process for alert list process
  - Attachment D: Internal NSA Email
  - Attachment E: NSA Inspector General Report
  - Attachment F: Letter from the NSA Inspector General
  - Attachment G: NSA, Signals Intelligence Directorate Office of Oversight and Compliance Response to the IG Report
  - Attachment H-J: Withheld from Public Release

February 26, 2009 — Notice of Compliance Incident

*Memorandum of the Government providing the FISC with notice of additional compliance incidents identified during NSA's ongoing end-to-end review of the telephony metadata program.*

March 2, 2009 — Order from the Foreign Intelligence Court

*In light of the compliance incidents identified and reported by the Government, the FISC ordered NSA to seek Court approval to query the telephony metadata on a case-by-case basis, except where necessary to protect against an imminent threat to human life "until such time as the Government is able to restore the Court's confidence that the government can and will comply with the previously approved [Court] procedures for accessing such data."*

**Docket Number BR 09-06**

June 22, 2009 — Order

*In response to the Government's reporting of a compliance incident related to NSA's dissemination of certain query results discovered during NSA's end-to-end review, the FISC ordered the Government to report on a weekly basis, any disseminations of information from the metadata telephony program outside of NSA and provide further explanation of the incident in its final report upon completion of the end-to-end review.*

**Docket Number BR 09-09**

August 19, 2009 — Report of the United States with attachments:

*Report of the Government describing the compliance issues uncovered during NSA's end-to-end review, including an explanation for how the compliance issues were remedied. Attached to the Report are declarations of the value of the bulk telephony metadata program from the Directors of NSA and the FBI.*

June 25, 2009 — Implementation of the Foreign Intelligence Surveillance Court Authorized Business Records FISA

*NSA's end-to-end review of it's implementation of the FISC's authorization under Section 215.*

**Docket Number BR 09-13**

September 3, 2009 — Primary Order from the Foreign Intelligence Surveillance Court

*Order of the FISC renewing authorization for the bulk telephony metadata program, and no longer requiring NSA to seek FISC approval to query the telephony metadata program on a case-by-case basis.*

September 25, 2009 — Order Regarding Further Compliance Incidence from the Foreign Intelligence Surveillance Court

*In response to the Government's identification and notice to the FISC regarding improper dissemination of information related to an ongoing threat, the FISC ordered a hearing to inform the FISC of the scope and circumstances of the compliance incident.*

**Docket Number BR: 09-15**

November 5, 2009 — Supplemental Opinion and Order from the Foreign Intelligence Surveillance Court

*Supplemental Opinion and Order of the FISC reiterating Court ordered restrictions on NSA's handling of query results of the telephony metadata program, and directing the Government to provide the court with additional information regarding queries of the telephony metadata.*

- #declassified
- #section 215
- #civil liberties
- #FISC
- #FISA
- #Patriot Act
- #Compliance
- #Congressional Oversight
- #Judicial Oversight
- 5 months ago
- 30
- Permalink

Share

Short URL
http://tmblr.co/ZZQjsquI

TwitterFacebookPinterestGoogle+


Go to LinkPop-upView Separately

**Review Group on Intelligence and Communications Technologies Conducts Meetings with Privacy and Civil Liberties Experts and Information Technology Industry Experts**

**September 9, 2013**

Today, members of the Review Group on Intelligence and CommunicationsTechnologies met with more than a dozen privacy and civil liberties groups and experts to hear comments about how the review group should carry out its tasks. Participants discussed recommendations about how to respect the Intelligence Community's commitment to privacy and civil liberties and maintain the public trust.

In a separate meeting, the review group today met with information technology companies and experts. Participants discussed the foreign policy implications, including economic implications, of U.S. policy concerning intelligence and communications technology.

The meetings today are part of the Review Group's overall efforts to receive comments from the public on all matters that the President has asked it to examine. Comments can be provided via reviewgroup@dni.gov. The deadline for public submissions is October 4, 2013. Further information on public comments is available via IC on the Record.

---

On August 12, 2013 President Obama directed the establishment of the review group. While it is administratively housed at the Office of the Director of National Intelligence (ODNI), it is conducting an independent review and will report directly to the President.

The review group's task is to advise the President "on how, in light of advancements in technology, the United States can employ its technical collection capabilities in a way that optimally protects our national security and advances our foreign policy while respecting our commitment to privacy and civil liberties, recognizing our need to maintain the public trust, and reducing the risk of unauthorized disclosure."

- #Review Group
- #oversight
- #civil liberties
- 5 months ago
- 22
- Permalink

Share

Short URL
http://tmblr.co/ZZQjsquc

TwitterFacebookPinterestGoogle+


Go to LinkPop-upView Separately

**Statement by Director of National Intelligence James R. Clapper on Allegations of Economic Espionage**

**September 8, 2013**

It is not a secret that the Intelligence Community collects information about economic and financial matters, and terrorist financing.

We collect this information for many important reasons: for one, it could provide the United States and our allies early warning of international financial crises which could negatively impact the global economy. It also could provide insight into other countries' economic policy or behavior which could affect global markets.

Our collection of information regarding terrorist financing saves lives. Since 9/11, the Intelligence Community has found success in disrupting terror networks by following their money as it moves around the globe. International criminal organizations, proliferators of weapons of mass destruction, illicit arms dealers, or nations that attempt to avoid international sanctions can also be targeted in an effort to aid America's and our allies' interests.

What we do not do, as we have said many times, is use our foreign intelligence capabilities to steal the trade secrets of foreign companies on behalf of - or give intelligence we collect to - US companies to enhance their international competitiveness or increase their bottom line.

As we have said previously, the United States collects foreign intelligence - just as many other governments do - to enhance the security of our citizens and protect our interests and those of our allies around the world. The intelligence Community's efforts to understand economic systems and policies and monitor anomalous economic activities is critical to providing policy makers with the information they need to make informed decisions that are in the best interest of our national security.

James R. Clapper
Director of National Intelligence

Via DNI.gov

- #intelligence community
- #terrorism
- #finance
- #foreign intelligence
- #statement
- 5 months ago
- 14
- Permalink

Share

Short URL
http://tmblr.co/ZZQjsqu

TwitterFacebookPinterestGoogle+


Go to LinkPop-upView Separately

**ODNI STATEMENT on the Unauthorized Disclosure of NSA Cryptological Capabilities**

**September 6, 2013**

It should hardly be surprising that our intelligence agencies seek ways to counteract our adversaries' use of encryption. Throughout history, nations have used encryption to protect their secrets, and today, terrorists, cybercriminals, human traffickers and others also use code to hide their activities. Our intelligence community would not be doing its job if we did not try to counter that.

While the specifics of how our intelligence agencies carry out this cryptanalytic mission have been kept secret, the fact that NSA's mission includes deciphering enciphered communications is not a secret, and is not news. Indeed, NSA's public website states that its mission includes leading "the U.S. Government in cryptology … in order to gain a decision advantage for the Nation and our allies."

The stories published yesterday, however, reveal specific and classified details about how we conduct this critical intelligence activity. Anything that yesterday's disclosures add to the ongoing public debate is outweighed by the road map they give to our adversaries about the specific techniques we are using to try to intercept their communications in our attempts to keep America and our allies safe and to provide our leaders with the information they need to make difficult and critical national security decisions.

- #cybersecurity
- #NSA
- #New York Times
- #The Guardian
- #ProPublica
- #cryptology
- #cryptography
- #encryption
- #cybercrime
- 5 months ago
- 75
- Permalink

Share

Short URL
http://tmblr.co/ZZQjsqu

## About

Created at the direction of the President of the United States, **IC ON THE RECORD** provides immediate, ongoing and direct access to factual information related to the lawful foreign surveillance activities carried out by the U.S. Intelligence Community.

Follow @IContheRecord

---

**CONTENT CATEGORIES:**

- - Official Statements
- - Declassified Documents
- - Testimony
- - Speeches & Interviews
- - Fact Sheets
- - Oversight & Compliance
- - Video

---

**HOT TOPICS:**

- - Civil Liberties
- - FISA
- - FISC
- - Section 215
- - Section 702

---

**IN THEIR OWN WORDS:**

- - James Clapper, DNI
- - Keith Alexander, Dir. NSA
- - Robert Litt, GC, ODNI
- - John Inglis, Dep. Dir., NSA
- - Alex Joel, CLPO, ODNI

Search this site

This website is maintained by the Office of the Director of National Intelligence.